Rappel :

Pour deux entiers relatifs a et b, on dit que a est congru à b modulo 7, et on écrit $a \equiv b$ [7] lorsqu'il existe un entier relatif k tel que $a = b + 7k$.

1/ *Cette question constitue une restitution organisée de connaissances* :

a) Soient a, b, c des entiers relatifs.

Démontrer que : Si $a \equiv b$ [7] et $c \equiv d$ [7], alors $ac \equiv bd$ [7].

$a \equiv b\ [7] \Leftrightarrow a = b + 7k \Leftrightarrow a - b = 7k \Leftrightarrow a - b \equiv 0\ [7]$.

$c \equiv d\ [7] \Leftrightarrow c = d + 7k' \Leftrightarrow c - d = 7k' \Leftrightarrow c - d \equiv 0\ [7]$.

Or : $ac - bd = a(c - d) + ad - bd = a(c - d) + d(a - b) = a(7k') + d(7k) = 7(ak' + dk)$.

Comme $ak' + dk \in \mathbb{Z}$, on déduit : $ac - bd \equiv 0\ [7] \Leftrightarrow ac \equiv bd\ [7]$

b) En déduire que : Si a et b sont des entiers relatifs non nuls, si $a \equiv b$ [7], alors $a^n \equiv b^n$ [7], pour tout entier naturel n.

Démonstration par récurrence : Soit la proposition P_n : " $a \equiv b\ [7] \Rightarrow a^n \equiv b^n\ [7]$ ", avec $n \in \mathbb{N}^*$.

a) *Initialisation* :

Vérifions P_1 vraie, soit " $a \equiv b\ [7] \Rightarrow a \equiv b\ [7]$ ", ce qui est une évidence.

b) *Héritage* :

Soit P_n vraie (" $a \equiv b\ [7] \Rightarrow a^n \equiv b^n\ [7]$ "), peut-on en déduire P_{n+1} vraie (" $a \equiv b\ [7] \Rightarrow a^{n+1} \equiv b^{n+1}\ [7]$ " ?

D'après 1-a) : $a \equiv b\ [7]$ et $a^n \equiv b^n\ [7] \Rightarrow a.a^n \equiv b.b^n\ [7]$ soit $a^{n+1} \equiv b^{n+1}\ [7]$.

c) *Conclusion* :

On déduit P_n vraie pour tout entier naturel n non nul.

2/ Pour $a = 2$ puis pour $a = 3$, déterminer un entier relatif n non nul tel que $a^n \equiv 1$ [7].

Soit $a = 2$:

$2 \equiv 2\ [7] \Rightarrow 2^2 \equiv 4\ [7] \Rightarrow 2^3 \equiv 8\ [7]$, or $8 = 7 + 1$, d'où : $2^3 \equiv 1\ [7]$. On déduit $n = 3$.

$3 \equiv 3\ [7] \Rightarrow 3^2 \equiv 9\ [7] \Rightarrow 3^2 \equiv 2\ [7] \Rightarrow 3^3 \equiv 6\ [7] \Rightarrow 3^4 \equiv 18\ [7] \Rightarrow 3^4 \equiv 4\ [7] \Rightarrow 3^5 \equiv 12\ [7] \Rightarrow 3^5 \equiv 5\ [7]$,

$3^6 \equiv 15\ [7] \Rightarrow 3^6 \equiv 1\ [7]$. On déduit $n = 6$.

3/ Soit a un entier naturel non divisible par 7.

a) Montrer que $a^6 \equiv 1$ [7].

Soit la division euclidienne de a par 7 : $a = 7q + r$ $(r \neq 0)$. D'où $a \equiv r\ [7]$, dont on déduit $a^6 \equiv r^6\ [7]$.

Il suffit donc de vérifier que pour tous les restes $r \in \{1,2,3,4,5,6\}$ on obtient $r^6 \equiv 1\ [7]$ pour déduire $a^6 \equiv 1\ [7]$.

D'après 1-b) :

$1 \equiv 1\ [7] \Rightarrow 1^7 \equiv 1\ [7]$.

On a vu : $2 \equiv 2\ [7] \Rightarrow 2^3 \equiv 1\ [7] \Rightarrow (2^3)^2 \equiv 1\ [7] \Rightarrow 2^6 \equiv 1\ [7]$.

On a vu : $3 \equiv 3\ [7] \Rightarrow 3^6 \equiv 1\ [7]$.

$4 = 2^2$, donc $4^3 = 2^6 \Rightarrow 4^3 \equiv 1\ [7] \Rightarrow (4^3)^2 \equiv 1\ [7] \Rightarrow 4^6 \equiv 1\ [7]$.

$5 \equiv 5\ [7] \Rightarrow 5^2 \equiv 25\ [7] \Rightarrow 5^2 \equiv 4\ [7] \Rightarrow (5^2)^3 \equiv 4^3\ [7] \Rightarrow 5^6 \equiv 1\ [7]$ d'après ligne précédente.

$6 \equiv 6\ [7] \Rightarrow 6^2 \equiv 36\ [7] \Rightarrow 6^2 \equiv 1\ [7]$.

Remarque : On pouvait procéder plus rapidement à l'aide du *Petit Théorème de Fermat*.

Si p est un nombre premier et que a ne soit pas divisible par p, alors : $a^{p-1} \equiv 1\ [p]$.

Ici : $p = 7$ est premier, et a n'est pas divisible par 7, d'où : $a^6 \equiv 1\ [7]$.

b) On appelle *ordre* de a mod 7 (modulo) , noté k , le plus petit entier naturel non nul tel que $a^k \equiv 1$ [7] .

Montrer que le reste r de la division euclidienne de 6 par k vérifie $a^r \equiv 1$ [7] .

$6 = kp + r \Rightarrow a^6 = a^{kp+r} = (a^k)^p \times a^r$. Sachant $a^6 \equiv 1$ [7] et $a^k \equiv 1$ [7] , on déduit $a^r \equiv 1$ [7] .

En déduire que k divise 6 .

On a vu que k est le plus petit entier naturel non nul tel que $a^k \equiv 1$ [7] , or $6 = kp + r \Rightarrow r < k$.

Comme $a^r \equiv 1$ [7] , la seule possibilité est $r = 0$ (sinon ce serait lui le plus petit entier non nul).

$r = 0 \Leftrightarrow 6 = kp$, donc k est un diviseur de 6 .

Quelles sont les valeurs possibles de k ?

k diviseur de $6 \Rightarrow k \in \{1 , 2 , 3, 6\}$.

c) Donner l'*ordre* mod 7 de tous les entiers compris entre 2 et 6 .

On a vu :

$a = 2 \Rightarrow k = 3$

$a = 3 \Rightarrow k = 6$

$a = 4 \Rightarrow k = 3$

$a = 5 \Rightarrow k = 6$

$a = 6 \Rightarrow k = 2$

4/ A tout entier naturel n , on associe le nombre $A_n = 2^n + 3^n + 4^n + 5^n + 6^n$.

Montrer que $A_{2006} \equiv 6$ [7] .

$2006 = 668\times3 + 2 \Rightarrow 2^{2006} \equiv (2^3)^{668} \times 2^2$ [7] avec $2^3 \equiv 1$ [7] , d'où : $2^{2006} \equiv 4$ [7] .

$2006 = 668\times3 + 2 \Rightarrow 4^{2006} \equiv (4^3)^{668} \times 4^2$ [7] avec $4^3 \equiv 1$ [7] , d'où : $4^{2006} \equiv 16$ [7] $\Rightarrow 4^{2006} \equiv 2$ [7] .

De même :

$2006 = 334\times6 + 2 \Rightarrow 3^{2006} \equiv (3^6)^{334} \times 3^2$ [7] avec $3^6 \equiv 1$ [7] , d'où : $3^{2006} \equiv 9$ [7] $\Rightarrow 3^{2006} \equiv 2$ [7] .

$2006 = 334\times6 + 2 \Rightarrow 5^{2006} \equiv (5^6)^{334} \times 5^2$ [7] avec $5^6 \equiv 1$ [7] , d'où : $5^{2006} \equiv 25$ [7] $\Rightarrow 5^{2006} \equiv 4$ [7] .

Ainsi que :

$2006 = 1003\times2 \Rightarrow 6^{2006} \equiv (6^2)^{1003}$ avec $6^2 \equiv 1$ [7] , d'où : $6^{2006} \equiv 1$ [7] .

Au total : $A_{2006} = 2^{2006} + 3^{2006} + 4^{2006} + 5^{2006} + 6^{2006} \equiv 4 + 2 + 2 + 4 + 1$ [7] $\Rightarrow A_{2006} \equiv 13$ [7] .

On obtient bien $A_{2006} \equiv 6$ [7] .